I claim:

1. A method of production and distribution of asymetric public and private keys between a key generation centre and at least one user unit (DEC), said unit comprising a security module (SM), said method consisting in:
- generating certificates comprising a public key and a private key in a first cryptographic unit (KPG),
- coding the private key by means of a service key in the first cryptographic unit (KPG) and storing said private key in a key memory (KPS),
- when sending the keys to a user unit, extracting the keys from the key memory (KPS), composing the certification with the public key,
- decoding the corresponding private key by means of the service key in a cryptographic security module and coding it with a transport key of the user.

2. A method according to Claim 1, characterised in that the encrypted private key is received by the user unit (DEC) and transmitted to the security module (SM) containing the transport key for decoding and storing the private key.

3. A method according to Claim 1, characterised in that it consists in using several monolithic cryptographic unit to obtain a high speed coding module.

4. A method according to claim 1, characterised in that it consists in:
- coding the public key of the centre with the transport key and transmitting it to the user unit (DEC),
- receiving by the user unit, the encrypted public key and transmitting it to the security module (SM),
- decoding and storing the public key by means of the transport key inside the security module (SM).

5. A method according to claim 2, characterised in that it consists in:
- coding the public key of the centre with the transport key and transmitting it to the user unit (DEC),
- receiving by the user unit, the encrypted public key and transmitting it to the security module (SM),

- decoding and storing the public key by means of the transport key inside the security module (SM).

6. A method according to claim 3, characterised in that it consists in:

- coding the public key of the centre with the transport key and transmitting it to the user unit (DEC),
- receiving by the user unit, the encrypted public key and transmitting it to the security module (SM),
- decoding and storing the public key by means of the transport key inside the security module (SM).